

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

GUAVA LLC,

Plaintiff,

v.

Does 1-5,

Defendants.

CASE NO. 12-cv-8000

Judge: Hon. John W. Darrah

Magistrate Judge: Hon. Young B. Kim

**PLAINTIFF'S *EX PARTE* APPLICATION
FOR LEAVE TO TAKE EXPEDITED
DISCOVERY**

**PLAINTIFF'S *EX PARTE* APPLICATION FOR LEAVE TO TAKE EXPEDITED
DISCOVERY**

Plaintiff Guava, LLC, the owner of protected computer systems with respect to the computer hacking activities at issue in this case, respectfully requests that this Court grant it leave to serve limited, immediate discovery on third party Internet Service Providers ("ISPs") to determine the identities of the Doe Defendants and their co-conspirators. The Court should grant this motion because Plaintiff has a demonstrated need for expedited discovery, the request is fair, and *ex parte* relief is proper under the circumstances.

FACTUAL BACKGROUND

Plaintiff, the owner of protected computer systems, filed its Complaint against Doe Defendants alleging computer fraud and abuse, civil conspiracy, conversion and negligence arising from unlawful computer-based breaches. (*See* Complaint ("Compl."), ECF No. 1.) Defendants and their co-conspirators, without authorization, used hacked usernames/passwords to hack into, Plaintiff's protected computer systems. (Compl. ¶ 18.) Although Plaintiff does not know the true names of the Defendants or their co-conspirators, Plaintiff has identified the

Defendants and the co-conspirators by unique Internet Protocol (“IP”) addresses which correspond to Defendants and to the co-conspirators on the date and at the time of the Defendants and the co-conspirators’ association with hacking activity. (*See* Exhibit A.) All of this information was gathered by a computer technician using procedures designed to ensure that the information gathered about the Doe Defendants and their co-conspirators was accurate.

Plaintiff has identified the ISPs that provide Internet access to Defendants and their co-conspirators and that assigned the unique IP addresses to the same. (*See* Exhibit A.) When presented with an IP address and the date and time of the hacking activity, an ISP can identify the name and address of an account holder (*i.e.*, the ISP’s subscriber) because that information is contained in the ISP’s subscriber activity log files. ISPs typically keep log files of subscriber activities for only limited periods of time—sometimes for as little as weeks or even days—before erasing the data.

In addition, some ISPs lease or otherwise allocate certain IP addresses to unrelated, intermediary ISPs. Because lessor ISPs have no direct relationship (customer, contractual, or otherwise) with the end-user, they are unable to identify the Doe Defendants or the co-conspirators through reference to their user logs. The leasee ISPs, however, should be able to identify the Doe Defendants and their co-conspirators by reference to their own user logs and records.

ARGUMENT

The Court should grant this motion for two reasons: the Plaintiff has a need for expedited discovery, and *ex parte* relief is proper under the circumstances where there are no known Defendants with whom to confer and the discovery request is directed at a third party.

I. THE COURT HAS AUTHORITY TO GRANT *EX PARTE* RELIEF, PLAINTIFF HAS MADE A NECESSARY SHOWING OF NEED FOR EXPEDITED DISCOVERY, AND PLAINTIFF’S REQUEST IS FAIR

The Court has broad authority under the Federal Rules of Civil Procedure to manage the discovery process. *See, e.g.*, Fed. R. Civ. P. 26(d); *id.* 16(b)(3)(B); *id.* 16(c)(2)(F). Rule 26(d)(1) explicitly permits a party to seek discovery from any source before the parties have conferred when authorized by a court order. *Id.* 26(d)(1). The courts in this and other jurisdictions rely on considerations of need and fairness when deciding whether this early discovery is warranted. *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. O’Connor*, 194 F.R.D. 618, 623 (N.D. Ill. 2000); *accord Lamar v. Hammel*, No. 08-02-MJR-CJP, 2008 WL 370697, at *3 (S.D. Ill. Feb. 11, 2008); *see also Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273 (N.D. Cal. 2002) (granting expedited discovery under a “balance of hardships” analysis); *Texas Guaranteed Student Loan Corp. v. Deepinder Dhindsa*, 2010 U.S. Dist. LEXIS 65753, Case No. 10-00335 (E.D. Cal. 2010). Plaintiff has a need for expedited discovery because physical evidence of hacking will be destroyed with the passage of time; because hacking is ongoing and continuous, necessitating immediate relief; and because this suit cannot proceed without this information. At the same time, Plaintiff’s request does not offend traditional notions of fairness and practicality. Therefore, this Court should grant Plaintiff’s motion.

A. The Court Has Authority to Grant Plaintiff’s Motion

This Court has authority to grant an *ex parte* request for expedited discovery. Rule 26(d) gives judges broad power to determine the timing and sequence of discovery. Fed. R. Civ. P. 26(d); *see also Crawford-El v. Britton*, 523 U.S. 574, 598 (1998) (“Rule 26 vests the trial judge with broad discretion to tailor discovery narrowly and to dictate the sequence of discovery.”); *Platinum Mfg. Int’l, Inc. v. Uninet Imaging, Inc.*, No. 8:08-cv-310-T-27, 2008 WL 927558, at *1 (M.D. Fla. Apr. 4, 2008) (recognizing that “expedited discovery may be appropriate” but

denying expedited discovery where plaintiff failed to show good cause); *Arista Records LLC v. Does 1–7*, No. 3:08-CV-18, 2008 WL 542709, at *1 (M.D. Ga. Feb 25, 2008) (citing *Nassau Terminals, Inc. v. M/V Bering Sea*, No. 99-104-CIV-J-20C, 1999 WL 1293476, at *1 (M.D. Fla. July 1, 1999) (“The moving party . . . must show good cause for departing from the usual discovery procedures.”)); *Equidyne Corp. v. Does 1-21*, 279 F.Supp. 2d 481, 483 (D. Del. 2003) (district court granted expedited discovery motion to allow the plaintiff to identify unknown Defendants). Under the balancing test standard, a request for expedited discovery should be granted where a moving party can show that its need for expedited discovery outweighs the prejudice to the responding party. *Texas Guaranteed Student Loan Corp. v. Deepinder Dhindsa*, 2010 U.S. Dist. LEXIS 65753, No. 10-00335 (E.D. Cal. 2010); *See El Pollo Loco, S.A. de C.V. v. El Pollo Loco, Inc.*, 344 F.Supp.2d 986, 991 (S.D.Tex.2004), *citing* 8 C. Wright, A. Miller & R. Marcus, *Federal Practice and Procedure* § 2046 .1 (1994).

The Federal Rules rely on the discretion of trial judges to tailor the scope, manner, and timing of discovery to the needs of the case and ensure the just, speedy, and inexpensive administration of justice. *See, e.g.*, Fed. R. Civ. P. 16(b)(3)(B); *id.* 16(c)(2)(F) (setting forth a trial court’s power to manage discovery by modifying the timing and extent of discovery through scheduling and case management orders). Courts in the past have elected to rely on considerations of need and fairness in reviewing expedited discovery requests. *Merrill Lynch*, 194 F.R.D. at 623 (“Plaintiff must make . . . showing of the need for the expedited discovery. . . . Courts must also protect Defendantss from unfair expedited discovery.”); *see also Vance v. Rumsfeld*, No. 06-C-6964, 2007 WL 4557812, at *3 (N.D. Ill. Dec. 21, 2007) (balancing “[p]laintiffs’ need for information relevant to this litigation against the undeniable hurdles of gathering discovery in Iraq during wartime”); *accord Lamar*, 2008 WL 370697, at *3 (“This Court . . . will rely on considerations of need and fairness.”); *IRC, LP v. McLean*, No. 09-189-

JPG-CJP, 2009 WL 839043, at *2 (S.D. Ill. Mar. 31, 2009); *See Semitool*, 208 F.R.D. at 273, 276 (N.D. Cal. 2002) (“Good cause may be found where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party”)’ *see also UMG Recordings*, 64 Fed. R. Serv.3d 305 (Magistrate Judge Edward M. Chen perfectly lays out all of the issues, analyzes the application of rules to facts, and concludes that the plaintiff is entitled to leave to take immediate discovery). Plaintiff’s request meets both of the criteria for need and fairness, and thus, the Court should grant this motion.

B. Plaintiff Has Made a Necessary Showing of Need for Expedited Discovery

Plaintiff has a need for expedited discovery of the identities of Doe Defendants and their co-conspirators because the physical evidence will be destroyed with the passage of time; because hacking is ongoing and continuous, necessitating immediate relief to prevent irreparable harm to Plaintiff; and because this suit cannot proceed without this information.

First, time is of the essence here because ISPs typically retain user activity logs containing the information sought by Plaintiff for only a limited period of time before erasing the data. If that information is erased, Plaintiff will have no ability to identify the Defendants and their co-conspirators, and thus will be unable to pursue its lawsuit to seek damages for unauthorized access of its protected content and prevent future unauthorized access. Other federal courts did not hesitate to grant motions for expedited discovery under similar circumstances, where “physical evidence may be consumed or destroyed with the passage of time, thereby disadvantaging one or more parties to the litigation.” *See, e.g., Living Scriptures v. Doe(s)*, No. 10-cv-0182-DB, 2010 WL 4687679, at *1 (D. Utah Nov. 10, 2010) (granting motion for expedited discovery where the information sought by plaintiff was “transitory in nature”); *Interscope Records v. Does 1–14*, No. 07-4107-RD, 2007 WL 2900210, at *1 (D. Kan. Oct. 1, 2007) (granting immediate discovery from ISPs because “the physical evidence of the alleged

[Defendant's] identity and incidents ... could be destroyed to the disadvantage of plaintiffs"); *Pod-Ners, LLC v. Northern Feed & Bean of Lucerne Ltd.*, 204 F.R.D. 675, 676 (D. Colo. 2002) (granting emergency motion for expedited discovery where "[f]urther passage of time . . . makes discovery . . . unusually difficult or impossible").

Second, because hacking is ongoing and continuous, Plaintiff needs to discover the identities of Doe Defendants and his co-conspirators to take quick actions to prevent further irreparable harm. Without a way to contact the Defendants or the co-conspirators, Plaintiff will continue to suffer ongoing, continuous injury due to their illegal activities.

Third, courts regularly grant expedited discovery where such discovery will "substantially contribute to moving th[e] case forward." *Semitoool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 275–76 (N.D. Cal. 2002); *see also Living Scriptures*, 2010 WL 4687679, at *1 (granting motion for expedited discovery of Doe Defendants because "without such information this case cannot commence")/ *Tracfone Wireless, Inc. v. King Trading, Inc.*, No. 3-08-CV-0398-B, 2008 WL 9182343 (N.D. Texas 2008) (allowing expedited discovery because it was almost impossible to obtain and preserve evidence without expedited discovery).

Here, the present lawsuit simply cannot proceed without discovering the identities of the Defendants and their co-conspirators. Although Plaintiff's forensic consultant was able to observe Defendants and their co-conspirators' hacking activity, the observations did not allow Plaintiff to access the Defendants or the co-conspirators' computers to obtain identifying information. Nor does the information available to Plaintiff allow it to upload a file onto the Defendants or the co-conspirators' computers or communicate with them in a manner that would provide notice of suit. Hence, the Plaintiff needs the Defendants and the co-conspirators' actual contact information to be able to communicate with them and name them in this lawsuit.

C. Plaintiff's Request is Both Fair and Practicable

Finally, discovery of the Defendants and the co-conspirators' identities does not frustrate notions of fairness and practicality. *Lamar*, 2008 WL 370697, at *3 (discussing whether information is readily available and the breadth and specificity of the discovery request as factors). The request is fair because Plaintiff's request is limited to basic contact information which is readily obtainable from ISPs; because Defendants and their co-conspirators have diminished expectations of privacy; and because the First Amendment does not shield the conduct that Defendants and their co-conspirators are alleged to have undertaken.

1. Discovery is fair and practical because Plaintiff's request is limited

The information requested by the Plaintiff is limited to basic contact information of the Defendants and their co-conspirators. The Plaintiff intends to use the information disclosed pursuant to their subpoenas only for the purpose of protecting its rights under Federal and state laws. *See Warner Bros. Records v. Does 1-14*, No. 8:07-CV-625-T-24, 2007 WL 4218983, at *1-2 (M.D. Fla. Nov. 29, 2007) ("Significantly, the only discovery that is being permitted prior to the Rule 26 conference is the production of information that may lead to the identity of the Does. It is reasonable to carry out this very limited discovery before the Rule 26 process begins.") The information is readily obtainable from the ISPs and the disclosure of personally identifying information by the cable providers was contemplated by Congress nearly three decades ago in the Cable Communications Policy Act of 1984, Pub. L. 98-549, § 2, 98 Stat. 2794 (codified as amended at 47 U.S.C. § 551 (2001)). Cable operators may disclose such information when ordered to do so by a court. § 551(c)(2)(B) (2001). The Act also requires the ISP to notify each subscriber about whom disclosure is sought about the subpoena and thus providing them with a notice of a pending action and an opportunity to appear and object. *Id.*

2. Discovery is fair because Defendants and their co-conspirators have diminished expectations of privacy

Defendants and their co-conspirators have little expectation of privacy because they have diminished these expectations by using hacked usernames/passwords to access Plaintiff's protected computer systems. Courts have repeatedly rejected privacy objections to discovery of personal contact information in cases involving computer crimes, concluding that Defendants in these cases have minimal expectations of privacy. *See, e.g., Arista Records, LLC v. Doe 3*, 604 F.3d 110, 118–19 (2d Cir. 2010) (concluding that plaintiff's need for discovery of identity outweighed Defendant's First Amendment right to anonymity); *Sony Music Entertainment Inc. v. Does 1–40*, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004) (“[D]efendants’ First Amendment right to remain anonymous must give way to plaintiffs’ right to use the judicial process to pursue what appear to be meritorious ... claims.”). Courts in many jurisdictions have also rejected challenges to disclosure of personally identifiable information based on privacy provisions of Family Educational Rights and Privacy Act (“FERPA”) where Defendants are students. *See, e.g., Fonovisa, Inc. v. Does 1–9*, No. 07-1515, 2008 WL 919701, *7–*8 (W.D. Pa. Apr. 3, 2008) (concluding that 20 U.S.C. § 1232g(b)(2) expressly authorizes disclosure of “directory information” such as name, address, and phone number; and that a MAC address does not fall within the purview of FERPA at all); *Arista Records LLC v. Does 1–4*, 589 F. Supp. 2d 151, 153 (D. Conn. 2008) (same); *Arista Records, L.L.C. v. Does 1–11*, 1:07CV2828, 2008 WL 4449444, at *3 (N.D. Ohio Sept. 30, 2008).

In addition, the courts have held that Internet subscribers do not have an expectation of privacy in their subscriber information, as they have already conveyed such information to their Internet Service Providers. *See, e.g., Guest v. Leis*, 255 F.3d 325, 335–36 (6th Cir. 2001) (“Individuals generally lose a reasonable expectation of privacy in their information once they

reveal it to third parties.”); *United States v. Hambrick*, Civ. No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000) (a person does not have a privacy interest in the account information given to the ISP in order to establish an email account); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (Defendant’s Fourth Amendment rights were not violated when an ISP turned over his subscriber information, as there is no expectation of privacy in information provided to third parties). Where federal privacy statutes authorize disclosure pursuant to a court order, courts have held that a plaintiff must make no more than a showing of relevance under the traditional standards of Rule 26. *See Laxalt v. McClatchy*, 809 F.2d 885, 888 (D.C. Cir. 1987); *see also In re Gren*, 633 F.2d 825 n.3 (9th Cir. 1980) (“court order . . . [only requires] good faith showing that the consumer records sought are relevant.”)

And finally, as one court aptly noted, “if an individual subscriber opens his computer to permit others . . . to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world.” *In re Verizon Internet Services, Inc.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003), *rev’d on other grounds, Recording Indus. Ass’n of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003).

3. Discovery is fair because the First Amendment is not a shield to commit computer crimes and torts

The First Amendment does not bar the disclosure of Defendants and their co-conspirators’ identities, either, because anonymous speech, like speech from identifiable sources, does not have absolute protection. The First Amendment does not protect the use of computers to hack into computer systems, and the Supreme Court, accordingly, has rejected First Amendment challenges to actions based on such conduct. *See, e.g., Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 555–56, 569 (1985). It is also well established in federal

courts that a person hacking into and removing protected content without authorization is not entitled to have their identity protected from disclosure under the First Amendment—limited protection afforded such speech gives way in the face of a *prima facie* showing of claims arising from computer misuse. *See Interscope Records v. Does 1–14*, 558 F. Supp. 2d 1176, 1178 (D. Kan. 2008); *see also Arista Records, Arista Records LLC v. Does 1–19*, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) (“[C]ourts have routinely held that a Defendant’s First Amendment privacy interests are exceedingly small where the ‘speech’” involves theft using a computer); *Sony Music*, 326 F. Supp. 2d at 566 (“[D]efendants have little expectation of privacy in downloading and distributing copyrighted songs without permission.”); *Arista Records, LLC v. Doe No. 1*, 254 F.R.D. 480, 481 (E.D.N.C. 2008).

Here, Plaintiff has alleged a *prima facie* case of violations of the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 . (See Compl. ¶¶ 25–33) and the other state law claims set forth in the Complaint. Thus, the limited protection afforded to Defendants and their co-conspirators by the First Amendment must give way to Plaintiff’s need to enforce its rights.

In summary, the Court has well-established authority to authorize expedited discovery of the Doe Defendants and the co-conspirators’ identities based on a showing of need. Plaintiff has made this showing of need because evidence of the identities of the hackers may soon be destroyed; because Plaintiff is suffering ongoing, continuous injury from Defendants’ hacking activities; and because this information is necessary for this action to continue. The discovery of this information is both fair and practicable because it is readily obtainable from the ISPs; because Defendants and their co-conspirators will get a notice and have an opportunity to appear and object; because Defendants and their co-conspirators have diminished expectations of privacy; and because the First Amendment does not bar disclosure of Defendants or their co-

conspirators' identities when they engage in computer hacking. For these reasons, the Court should grant Plaintiff's motion for expedited discovery. This *ex parte* relief is also appropriate because the discovery is necessary to identify Doe Defendants and their co-conspirators.

II. EX PARTE RELIEF IS APPROPRIATE UNDER THE CIRCUMSTANCES

Ex parte relief is appropriate under the circumstances where there are no known defendants with whom to confer. Courts routinely and virtually universally allow *ex parte* discovery to identify "Doe" Defendants. *See, e.g., Maclin v. Paulson*, 627 F.2d 83, 87 (7th Cir. 1980) (reversing and remanding because when "a party is ignorant of Defendants' true identity . . . plaintiff should have been permitted to obtain their identity through limited discovery") (citing *Owens v. Haas*, 601 F.2d 1242, 1247 (2d Cir. 1979); *Gordon v. Leeke*, 574 F.2d 1147, 1152–53 (4th Cir. 1978)); *see also Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (error to dismiss unnamed Defendants given possibility that identity could be ascertained through discovery) (citing *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980) ("[W]here the identity of the alleged Defendant [is] not [] known prior to the filing of a complaint . . . the plaintiff should be given an opportunity through discovery to identify the unknown Defendants."); *Dean v. Barber*, 951 F.2d 1210, 1215 (11th Cir. 1992) (holding that the district court erred when it denied the plaintiff's motion to join John Doe Defendants where identity of John Doe could have been determined through discovery).

Courts across the country have applied the same principles to *ex parte* expedited discovery in suits that are factually similar to this one. *See, e.g., Warner Bros. Record Inc. v. Does 1–14*, 555 F. Supp. 2d 1, 1–2 (D.D.C. 2008) (granting *ex parte* motion for immediate discovery on an ISP seeking to obtain the identity of each Doe Defendants by serving a Rule 45 subpoena); *Arista Records LLC v. Does 1–7*, No. 3:08-CV-18(CDL), 2008 WL 542709, at *1 (M.D. Ga. Feb. 25, 2008) (same); *Arista Records LLC v. Does 1–43*, No. 07cv2357-LAB (POR),

2007 WL 4538697, at *1 (S.D. Cal. Dec. 20, 2007) (same); *Warner Bros. Records, Inc. v. Does I–20*, No. 07-CV-1131, 2007 WL 1655365, at *2 (D. Colo. June 5, 2007) (same). This Court should follow the well-established precedent and permit *ex parte* discovery of the Doe Defendants and their co-conspirators' identities. As in the cases cited above, the Doe Defendants and their co-conspirators' identities are not known, but can be discovered through limited discovery.

Further, *ex parte* relief is appropriate because Plaintiff is not requesting an order compelling Defendants or their co-conspirators to respond to particular discovery, where notice and opportunity to be heard would be of paramount significance to the other party. Rather, Plaintiff is merely seeking an order authorizing it to commence limited discovery directed towards a third party. For these reasons, an *ex parte* motion to discover the identities of Doe Defendants and their co-conspirators is appropriate and the Court should grant Plaintiff's motion.

CONCLUSION

The Court should grant Plaintiff's motion for two reasons. First, Plaintiff has a need for expedited discovery because physical evidence of the identity of the Doe Defendants and the co-conspirators may be destroyed with the passage of time; because hacking is ongoing and continuous, necessitating immediate relief; and because this suit cannot proceed without this information. The discovery is fair and practicable because Plaintiff's request is limited and the information is easily obtainable from third parties; because Defendants and their co-conspirators have diminished expectations of privacy; and because First Amendment does not provide a license to hack into websites. Second, *ex parte* relief is proper under the circumstances where there are no known Defendants with whom to confer. Therefore, Plaintiff respectfully asks the Court to grant this motion and enter an Order substantially in the form of the attached Proposed Order.

Respectfully submitted,

Guava, LLC

DATED: October 17, 2012

By: /s/ Paul Duffy
Paul Duffy (Bar No. 6210496)
Prenda Law Inc.
161 N. Clark St., Suite 3200
Chicago, IL 60601
Telephone: (312) 880-9160
Facsimile: (312) 893-5677
E-mail: paduffy@wefightpiracy.com
Attorney for Plaintiff